ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 9735-5– 2012

ЭЛЕКТРОННЫЙ ОБМЕН ДАННЫМИ В УПРАВЛЕНИИ, ТОРГОВЛЕ И НА ТРАНСПОРТЕ (EDIFACT)

Синтаксические правила для прикладного уровня (версия 4, редакция 1)

Часть 5

Правила защиты для пакетного ЭОД (аутентичность, целостность и неотказуемость источника)

ISO 9735-5:2002
Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)
(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Проспект» совместно с Ассоциацией автоматической идентификации «ЮНИСКАН/ГС1 РУС» на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 55 «Терминология, элементы данных и документация в бизнес-процессах и электронной торговле»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 ноября 2012 г. № 975-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 9735-5:2002 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 5. Правила защиты для пакетного ЭОД[1)] (аутентичность, целостность и неотказуемость источника)» (ISO 9735-5:2002 «Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru).

Стандартинформ, 2014

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

[1)] ЭОД – электронный обмен данными соответствует английскому EDI – electronic data interchange.

Содержание

1 Область применения 1
2 Соответствие стандарту 1
3 Нормативные ссылки 1
4 Термины и определения 2
5 Правила использования групп сегментов заголовка и окончания защиты для пакетного ЭОД 2
6 Правила использования групп сегментов заголовка и окончания защиты обмена и группы для пакетного ЭОД 9
Приложение А (справочное) Угрозы безопасности EDIFACT и технические решения проблемы 12
Приложение В (справочное) Способы защиты структуры EDIFACT 15
Приложение С (справочное) Примеры защиты сообщений 17
Приложение D (справочное) Функции фильтрации для наборов графических знаков UN/EDIFACT уровней А и С 26
Приложение Е (справочное) Службы и алгоритмы защиты 28
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации 35
Библиография 36

Введение

Настоящий стандарт включает в себя правила прикладного уровня для структурирования данных в рамках обмена электронными сообщениями в открытой среде, с учетом требований пакетной или интерактивной обработки. Эти правила утверждены Европейской экономической комиссией Организации Объединенных Наций (UN/ECE) в качестве синтаксических правил электронного обмена данными в управлении, торговле и на транспорте (EDIFACT) и являются частью «Справочника по обмену торговыми данными Организации Объединенных Наций» (UNTDID[1)]), который содержит также рекомендации по разработке сообщений пакетного и интерактивного обмена.

Спецификации и протоколы связи не входят в область распространения настоящего стандарта.

Настоящий стандарт входит в комплекс стандартов ИСО 9735 и обеспечивает возможность организации дополнительной защиты пакетных структур данных EDIFACT, таких как сообщения, пакеты, группы или обмен.

Комплекс стандартов ИСО 9735 состоит из следующих частей, имеющих общий подзаголовок «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1)»:

— часть 1. Синтаксические правила, общие для всех частей;

— часть 2. Синтаксические правила, специфичные для пакетного ЭОД;

— часть 3. Синтаксические правила, специфичные для интерактивного ЭОД;

— часть 4. Сообщение синтаксического и служебного уведомления для пакетного ЭОД (тип сообщения — CONTRL);

— часть 5. Правила защиты для пакетного ЭОД (аутентичность, целостность и неотказуемость источника);

— часть 6. Сообщение для защищенной аутентификации и защищенного квитирования (тип сообщения — AUTACK);

— часть 7. Правила защиты для пакетного ЭОД (конфиденциальность);

— часть 8. Ассоциированные данные в ЭОД;

— часть 9. Сообщение для управления ключами и сертификатами защиты (тип сообщения — KEYMAN);

— часть 10. Справочники служебных синтаксических структур.

[1)] UNTDID – United Nations Trade Data Interchange Directory.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЭЛЕКТРОННЫЙ ОБМЕН ДАННЫМИ В УПРАВЛЕНИИ, ТОРГОВЛЕ И НА ТРАНСПОРТЕ (EDIFACT)
Синтаксические правила для прикладного уровня
(версия 4, редакция 1)
Часть 5
Правила защиты для пакетного ЭОД (аутентичность, целостность и неотказуемость источника)

Electronic data interchange for administration, commerce and transport (EDIFACT) —
Application level syntax rules
(Syntax version number: 4, Syntax release number: 1) —
Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

Дата введения – 2014 – 01 – 01

1 Область применения

Настоящий стандарт устанавливает синтаксические правила защиты EDIFACT и определяет метод защиты на уровне сообщений/пакетов, групп и обмена для обеспечения их аутентичности, целостности и неотказуемости источника в соответствии с принятыми механизмами защиты.

2 Соответствие стандарту

Для соответствия обмена настоящему стандарту в обязательном элементе данных 0002 (номер версии синтаксических правил) следует использовать номер версии "4", а в условном элементе данных 0076 (номер редакции синтаксических правил) должен быть указан номер редакции "01". Каждый из этих элементов данных входит в сегмент UNB (заголовок обмена). В обменах, в которых продолжает использоваться синтаксис более ранних версий, для различения соответствующих синтаксических правил, необходимо указывать следующие номера версий:

ИСО 9735:1988 – номер версии синтаксических правил: 1;

ИСО 9735:1988 (с изменениями, принятыми в 1990 г.) – номер версии синтаксических правил: 2;

ИСО 9735:1988 (с изменением 1, принятым в 1992 г.) – номер версии синтаксических правил: 3;

ИСО 9735:1998 – номер версии синтаксических правил: 4.

Соответствие стандарту означает, что выполнены все его требования, включая все опции. Если же поддерживаются не все опции, то в любом заявлении о соответствии должно содержаться положение, идентифицирующее опции, по которым декларируется соответствие.

Данные, используемые в обмене, признаются соответствующими настоящему стандарту, если их структура и представление отвечают синтаксическим правилам, определенным в настоящем стандарте.

Устройства, поддерживающие настоящий стандарт, признаются соответствующими ему, если эти устройства способны формировать и/или интерпретировать данные, структурированные и представленные в соответствии с требованиями настоящего стандарта.

Соответствие настоящему стандарту включает в себя также соответствие частям 1, 2, 8 и 10 комплекса стандартов ИСО 9735.

Положения стандартов, указанных в настоящем стандарте, являются составными элементами критериев соответствия настоящему стандарту.

3 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие нормативные документы, положения которых необходимо учитывать при использовании настоящего стандарта. В случае ссылок на документы, у которых указана дата утверждения, необходимо пользоваться только указанной редакцией. В случае, когда дата утверждения не приведена, следует пользоваться последней редакцией ссылочных документов, включая любые поправки и изменения к ним.

ИСО 9735-1:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 1.

Синтаксические правила, общие для всех частей (ISO 9735-1:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 1: Syntax rules common to all parts)

ИСО 9735-2:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 2. Синтаксические правила, специфичные для пакетного ЭОД (ISO 9735-2:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 2: Syntax rules specific to batch EDI)

ИСО 9735-6:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 6. Сообщение для защищенной аутентификации и защищенного квитирования (тип сообщения — AUTACK) (ISO 9735-6:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 6: Secure authentication and acknowledgement message (message type — AUTACK))

ИСО 9735-7:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 7. Правила защиты для пакетного ЭОД (конфиденциальность) (ISO 9735-7:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 7: Security rules for batch EDI (confidentiality))

ИСО 9735-8:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 8. Ассоциированные данные в ЭОД (ISO 9735-8:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 8: Associated data in EDI)

ИСО 9735-10:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 10. Справочники служебных синтаксических структур (ISO 9735-10:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 10: Syntax service directories)

ИСО/МЭК 10181-2:1996 Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы аутентификации (ISO/IEC 10181-2:1996 Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework)

ИСО/МЭК 10181-4:1997 Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы неотказуемости (ISO/IEC 10181-4:1997, Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework)

ИСО/МЭК 10181-6:1996 Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы целостности (ISO/IEC 10181-6:1996, Information technology — Open Systems Interconnection — Security frameworks for open systems: Integrity framework)

4 Термины и определения

В настоящем стандарте применены термины, определенные в ИСО 9735-1.

5 Правила использования групп сегментов заголовка и окончания защиты для пакетного ЭОД

5.1 Защита на уровне сообщений/пакетов (встроенная защита сообщений и пакетов)

5.1.1 Общие положения

Угрозы безопасности, свойственные процессам передачи сообщений/пакетов, и связанные с ними службы защиты приведены в приложениях А и В.

В данном подразделе представлена структура системы защиты EDIFACT на уровне сообщений/пакетов.

Службы защиты, рассмотренные в настоящем стандарте, должны предоставляться применительно к любому существующему сообщению путем включения групп сегментов заголовка защиты и групп сегментов окончания защиты после сегмента UNH и перед сегментом UNT, а применительно к любому существующему пакету – путем включения указанных групп сегментов после сегмента UNO и перед сегментом UNP.

5.1.2 Группы сегментов заголовка и окончания защиты

На рисунке 1 приведено схематическое представление обмена, иллюстрирующее защиту на уровне сообщений.

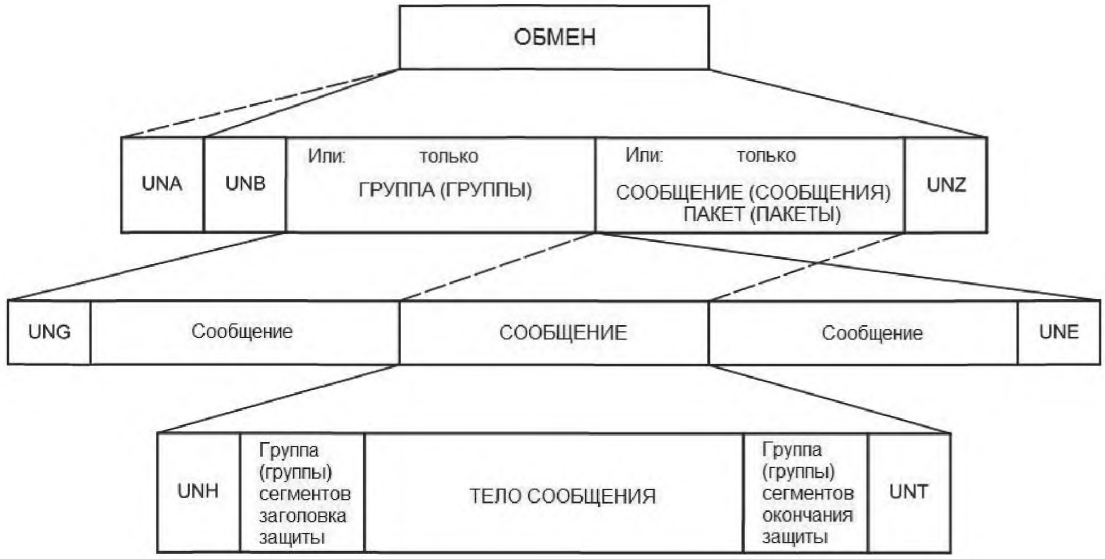

Рисунок 1 – Схематическое представление обмена, показывающее службы с защитой на уровне сообщений

На рисунке 2 приведено схематическое представление обмена, иллюстрирующее защиту на уровне пакетов.

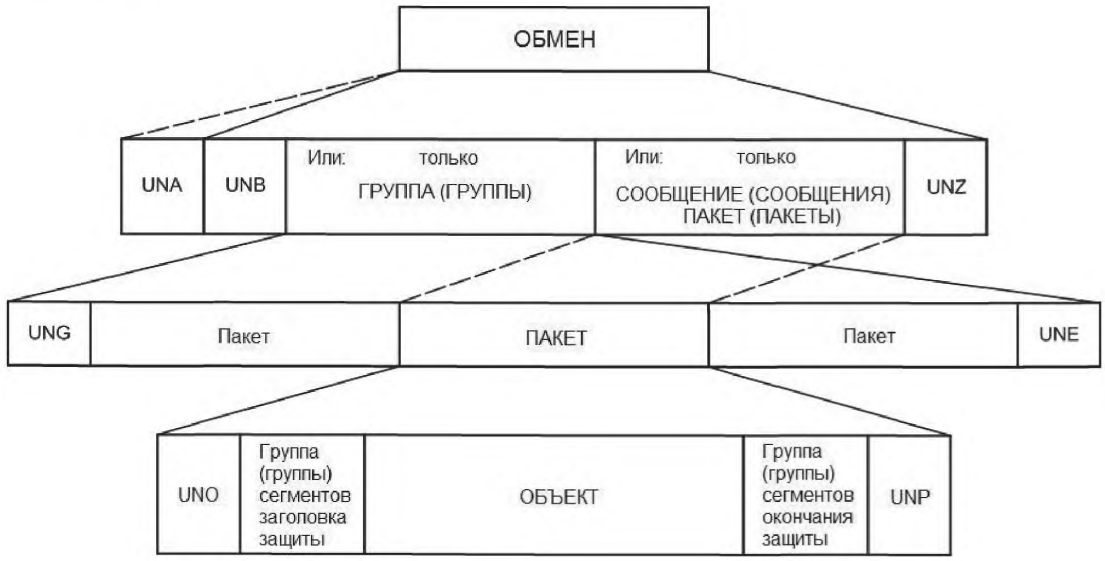

Рисунок 2 – Схематическое представление обмена, показывающее службу с защитой на уровне пакетов

5.1.3 Структура групп сегментов заголовка и окончания защиты

Таблица 1 – Группы сегментов заголовка защиты и окончания защиты (служба защиты на уровне сообщений)

ТЕГ	Наименование	S	R	
UNH	Заголовок сообщения	M	1	
-----	Группа сегментов 1 ----------	C	99	--------+
USH	Заголовок защиты	M	1	I
USA	Алгоритм защиты	C	3	I
-----	Группа сегментов 2 ----------	C	2	----+ I
USC	Сертификат	M	1	I I
USA	Алгоритм защиты	C	3	I I
USR	Результат защиты	C	1	--------+
	Тело сообщения			
-----	Группа сегментов n ----------	C	99	----+
UST	Окончание защиты	M	1	I
USR	Результат защиты	C	1	----+
UNT	Окончание сообщения	M	1	

Таблица 2 – Группы сегментов заголовка защиты и окончания защиты (служба защиты на уровне пакетов)

ТЕГ	Наименование	S	R	
UNO	Заголовок объекта	M	1	
-----	Группа сегментов 1 ----------	C	99	--------+
USH	Заголовок защиты	M	1	I
USA	Алгоритм защиты	C	3	I
-----	Группа сегментов 2 ----------	C	2	----+ I
USC	Сертификат	M	1	I I
USA	Алгоритм защиты	C	3	I I
USR	Результат защиты	C	1	--------+
	Объект			
-----	Группа сегментов n ----------	C	99	----+
UST	Окончание защиты	M	1	I
USR	Результат защиты	C	1	----+
UNP	Окончание объекта	M	1	

Примечание – Полное описание сегментов и элементов данных, включая сегменты заголовка сообщения UNH, окончания сообщения UNT, заголовка объекта UNO и окончания объекта UNP приведено в ИСО 9735-10. В настоящем стандарте они не детализируются.

5.1.4 Детализация сегмента данных

Группа сегментов 1: USH-USA-SG2 (группа сегментов заголовка защиты)

Группа сегментов, идентифицирующая службу защиты и применяемые механизмы защиты и содержащая данные, необходимые для выполнения вычислений, связанных с контролем достоверности.

В рамках одного сообщения/пакета могут существовать несколько различных групп сегментов заголовка защиты, когда к одному сообщению/пакету могут быть применены разные службы защиты (например, обеспечения целостности и неотказуемости источника) или одна и та же служба защиты может использоваться несколькими участниками обмена данными.

USH – заголовок защиты

Сегмент, определяющий службу защиты, используемую для сообщения/пакета, в которые этот сегмент включен.

В этом сегменте могут идентифицироваться стороны, вовлеченные в службу защиты (отправитель и адресат элементов защиты), если только они не определены в явной форме сертификатами (сегмент USC) при использовании асимметричных алгоритмов защиты.

Составной элемент данных S500, содержащий подробные сведения для идентификации службы защиты, должен присутствовать в сегменте USH в следующих случаях:

- при использовании симметричных алгоритмов или
- при использовании асимметричных алгоритмов, когда имеются два сертификата; элемент S500 в этой ситуации позволяет различать сертификаты отправителя и адресата.

В последнем случае идентификатор участвующей стороны в элементе S500 (которым может быть любой из элементов данных S500/0511, S500/0513, S500/0515, S500/0586) должен быть тем же, что и идентификатор стороны, определенной как «владелец сертификата» в одном из элементов S500, присутствующих в составе сегмента USC из группы сегментов 2, а элемент данных S500/0577 должен указывать функцию участвующей стороны (отправитель или адресат).

Элемент данных «имя ключа» в составном элементе данных для идентификации службы защиты (S500/0538) может использоваться для установления зависимости между ключами отправляющей и принимающей сторон.

Эта зависимость может быть установлена с помощью простого элемента данных идентификатора ключа длясоставного элемента данных параметра алгоритма защиты (S503/0554) в сегменте USA группы сегментов 1.

Элемент данных S500/0538 в сегменте USH может использоваться в тех случаях, когда нет необходимости передавать сегмент USA в группе сегментов 1 (поскольку криптографические механизмы были предварительно согласованы между партнерами).

Рекомендуется использовать либо элемент данных S500/0538 в сегменте USH, либо элемент данных S503/0554 с надлежащим квалификатором в сегменте USA, но не оба этих элемента данных вместе в рамках одной и той же группы сегментов заголовка.

Сегмент USH может определять функцию фильтрации, используемую применительно к двоичным полям сегмента USA внутри группы сегментов 1 и сегмента USR соответствующей группы сегментов окончания защиты.

Сегмент USH может содержать порядковый номер защиты, используемый для обеспечения целостности данных, и дату создания элементов защиты.

Сегмент USA – алгоритм защиты

Этот сегмент идентифицирует алгоритм защиты и метод его использования, а также содержит требуемые для этого технические параметры. Используемый алгоритм применяют непосредственно к сообщению или пакету. Это может быть симметричный алгоритм шифрования, хеш-функция или алгоритм сжатия. Например, применительно к цифровой подписи сегмент USA указывает используемую функцию хеширования, зависящую от конкретного сообщения.

Асимметричные алгоритмы не следует вызывать непосредственно в этом сегменте USA группы сегментов 1; они могут присутствовать только внутри группы сегментов 2, инициируемой сегментом USC.

Допускается использовать три вхождения сегмента USA. Одно вхождение следует использовать для симметричного алгоритма или хеш-функции, которые требуются для реализации службы защиты, определенной в сегменте USH. Описание двух других вхождений приведены в ИСО 9735-7.

При необходимости допускается использовать индикацию механизма дополнения незначащими битами.

Группа сегментов 2: USC-USA-USR (группа сертификата)

Эта группа сегментов содержит данные, необходимые для контроля подлинности методов защиты сообщений/пакетов в случае применения асимметричных алгоритмов. Группу сегментов сертификата применяют для идентификации пары асимметричных ключей, даже в том случае, если сертификаты не используются.

Для однозначной идентификации пары используемых асимметричных ключей необходимо наличие в сегменте USC либо полной группы сегментов сертификата (включая сегмент USR), либо только элементов данных. Наличия полного сертификата можно избежать, если обмен сертификатами между двумя сторонами уже произошел или если сертификат может быть извлечен из базы данных.

В случаях, когда принимают решение использовать сертификат, не относящийся к EDIFACT (например, X.509), его синтаксис и версия подлежат идентификации в элементе данных 0545 сегмента USC. Подобные сертификаты могут быть переданы в составе пакета EDIFACT.

Допускаются два вхождения группы сегментов USC-USA-USR. Одно вхождение имеет отношение к сертификату отправителя сообщения/пакета (этот сертификат будет использован получателем сообщения/пакета для проверки цифровой подписи отправителя); второе вхождение имеет отношение к сертификату получателя сообщения/пакета (запрашиваемому только по указателю сертификата), когда в целях сохранения конфиденциальности симметричных ключей отправитель использует открытый ключ получателя.

При наличии обоих вхождений в рамках одной группы сегментов заголовка защиты их различение обеспечивается составным элементом данных идентификационных элементов защиты (S500) совместно с элементом данных указателя сертификата (0536).

Данную группу сегментов не применяют, если асимметричный алгоритм не используется.

Сегмент сертификата USC

Сегмент, содержащий удостоверение владельца сертификата и идентифицирует орган сертификации, выдавший этот сертификат. Элемент данных, называемый функцией фильтрации (код 0505) должен указывать конкретную функцию фильтрации, применяемую к двоичным полям сегментов USA и сегмента USR внутри группы сегментов 2.

Сертификат USC может иметь два вхождения S500: одно – для владельца сертификата (идентифицирующее сторону, которая подписывается закрытым ключом, ассоциируемым с открытым ключом, содержащимся в данном сертификате), и второе – для идентификации издателя сертификата (органа сертификации).

Сегмент USA – алгоритм защиты

Сегмент, идентифицирующий алгоритм защиты и его техническую реализацию и содержащий необходимые технические параметры. Три разных вхождения сегмента USA в группе сегментов 2 идентифицируют:

1 алгоритм, использованный издателем сертификата при вычислении значения хеш-функции сертификата (функция хеширования);

2 алгоритм, использованный издателем сертификата для его изготовления (то есть для подписания результата применения хеш-функции к содержимому сертификата) (асимметричный алгоритм);

3a алгоритм, использованный отправителем для подписания сообщения/пакета (то есть для подписания результата применения описанной в сегменте USH хеш-функции к содержимому сообщения/пакета) (асимметричный алгоритм), либо

3b асимметричный алгоритм получателя, использованный отправителем для шифрования ключа, необходимого для работы симметричного алгоритма, который применяется к содержимому сообщения/пакета и запрашивается группой сегментов 1, активизируемой сегментом USH (асимметричный алгоритм).

При необходимости допускается приводить информацию о возможности применения механизма дополнения незначащими битами.

Сегмент USR – результат защиты

Сегмент, содержащий результат применения функций защиты сертификата органом сертификации. Этот результат должен представлять собой электронную подпись сертификата, сформированную органом сертификации путем заверения результата применения соответствующей хеш-функции к данным удостоверения.

Применительно к сертификату, формирование электронной подписи начинается с обработки первого знака сегмента USC (буквы “U”) и заканчивается обработкой последнего знака последнего сегмента USA (включая следующий за ним разделитель).

Группа сегментов n: UST-USR (группа окончания защиты)

Группа сегментов, содержащая ссылку на группу сегментов заголовка защиты и результат применения функций защиты к сообщению/пакету.

Сегмент UST – окончание защиты

Сегмент, устанавливающий связь между группой сегментов заголовка защиты и группой сегментов окончания защиты, а также определяющий суммарное число сегментов защиты, содержащихся в этих группах.

Сегмент USR – результат защиты

Сегмент, содержащий результат применения к сообщению/пакету функций защиты, которые заданы в связанной с ним группе заголовка защиты. В зависимости от механизмов защиты, определенных в связанной группе заголовка защиты, результатом применения может быть один из следующих:

- результат, вычисленный путем прямой обработки сообщения/пакета по алгоритму, определенному в сегменте USA внутри группы сегментов 1 из группы заголовка защиты, или

- результат, подтвержденный электронной подписью с помощью асимметричного алгоритма, который задан в сегменте USA внутри группы сегментов 2 из группы сегментов заголовка защиты, результат хеширования сообщения/пакета по алгоритму, определенному в сегменте USA внутри группы сегментов 1 из группы сегментов заголовка защиты.

5.1.5 Область защиты

Допускается использовать два варианта применения области защиты:

1. Вычисление каждого из значений параметров целостности и аутентификации, а также формирование цифровых подписей начинается с прямой обработки текущей группы сегментов заголовка защиты, тела сообщения или объекта. В этом случае область защиты не должна охватывать никакие другие группы сегментов заголовка или окончания защиты.

Отсчет знаков группы сегментов заголовка защиты следует начинать с его первого знака (от буквы “U”) и заканчивать разделителем включительно, следующим за этой группой сегментов, а тело сообщения или объект – с первого знака после разделителя, завершающего последнюю группу сегментов заголовка защиты, до разделителя, предшествующего первому знаку первой группы сегментов окончания защиты, включительно.

Таким образом, порядок, в котором осуществляются службы защиты, заранее не регламентируется, и они являются полностью независимыми друг от друга.

Рисунок 3 иллюстрирует этот случай (область применения служб защиты, определенная в заголовке защиты 2, выделена темно-серым цветом).

UNH/UNO	Группа 3 сегментов заголовка защиты	Группа 2 сегментов заголовка защиты	Группа 1 сегментов заголовка защиты	ТЕЛО СООБЩЕ-НИЯ/ ОБЪЕКТ	Группа 1 сегментов окончания защиты	Группа 2 сегментов окончания защиты	Группа 3 сегментов окончания защиты	UNT/UNP

Рисунок 3 – Схематическое представление области защиты (только группа сегментов заголовка защиты и тело сообщения/объекта)

2. Вычислительная обработка осуществляется, начиная с текущей группы сегментов заголовка защиты и заканчивая соответствующей группой сегментов окончания защиты включительно. В рассматриваемом случае область защиты должна охватывать текущую группу сегментов заголовка защиты, тело сообщения или объект, а также остальные вложенные группы сегментов заголовка и окончания защиты.

Эта область должна включать в себя каждый знак от первой буквы “U” текущей группы сегментов заголовка защиты до разделителя, предшествующего первому символу соответствующей группы сегментов окончания защиты, включительно.

Рисунок 4 иллюстрирует этот случай (область применения служб защиты, определенной в заголовке защиты 2, выделена темно-серым цветом).

UNH/UNO	Группа 3 сегментов заголовка защиты	Группа 2 сегментов заголовка защиты	Группа 1 сегментов заголовка защиты	ТЕЛО СООБЩЕ-НИЯ/ ОБЪЕКТ	Группа 1 сегментов окончанияз ащиты	Группа 2 сегментов окончанияз ащиты	Группа 3 сегментов окончания защиты	UNT/UNP

Рисунок 4 – Схематическое представление области защиты (от группы сегментов заголовка защиты до группы сегментов окончания защиты)

Для каждой добавляемой службы защиты допускается применять любой из вышеуказанных подходов.

В обоих случаях связь между группой сегментов заголовка защиты и соответствующей группой сегментов окончания защиты должна обеспечиваться элементами данных «справочный номер защиты» в сегментах USH и UST.

5.2 Принципы использования

5.2.1 Выбор служб защиты

Группа сегментов заголовка защиты может содержать в себе следующую общую информацию:

- применяемые службы защиты;
- идентификаторы взаимодействующих сторон;

- используемый механизм защиты;
- уникальный идентификатор (порядковый номер и/или отметка времени);
- требование неотказуемости приема.

Если для одной и той же структуры EDIFACT требуется больше одной службы защиты, то группа сегментов заголовка защиты может повторяться несколько раз. Это происходит при наличии нескольких пар взаимодействующих партнеров. Если несколько служб защиты необходимы для одной и той же взаимодействующей пары, эти службы могут быть включены в единственную пару групп сегментов заголовка и окончания защиты.

5.2.2 Аутентичность

При необходимости обеспечения аутентификации источника структуры EDIFACT, она должна обеспечиваться в соответствии с принципами, установленными стандартом ИСО/МЭК 10181-2 с использованием надлежащей пары групп сегментов заголовка и окончания защиты.

Служба защиты аутентификации источника должна быть определена в сегменте USH, а алгоритм – в сегменте USA группы сегментов 1; алгоритм должен быть симметричным.

Сторона, действующая как инициатор защиты, должна вычислить значение параметра аутентичности, которое должно быть передано в сегменте USR группы сегментов окончания защиты. Сторона, действующая как адресат защиты, должна провести проверку значения параметра аутентичности.

Эта служба может включать в себя службу обеспечения целостности и рассматриваться как промежуточный результат службы неотказуемости источника.

Если в основе практической реализации службы защиты аутентификации источника лежат аппаратные средства, надежно защищенные от внешних воздействий, или использован принцип третьих доверительных сторон, то такое техническое решение является примером реализации службы неотказуемости источника. Данный подход должен быть указан в соглашении об обмене.

5.2.3 Целостность

При необходимости обеспечения целостности содержимого структуры EDIFACT, это следует выполнять в соответствии с положениями, установленными ИСО/МЭК 10181-6 с использованием надлежащей пары групп сегментов заголовка и окончания защиты.

Служба защиты по обеспечению целостности должна быть определена в сегменте USH, а алгоритм – в сегменте USA группы сегментов 1; необходимо использовать хеш-функцию или симметричный алгоритм.

Сторона, действующая как инициатор защиты, должна вычислить значение параметра целостности, которое должно быть передано в сегменте USR группы сегментов окончания защиты. Сторона, действующая как адресат защиты, должна провести проверку значения параметра целостности.

Эта служба может рассматриваться как промежуточный результат–службы аутентификации источника или службы неотказуемости источника.

При необходимости обеспечения целостности цепочки структур EDIFACT в группе сегментов заголовка защиты должен присутствовать либо порядковый номер защиты, либо защитная отметка времени, либо то и другое, а также должна использоваться служба обеспечения целостности контента или служба аутентификации источника или служба неотказуемости источника.

5.2.4 Неотказуемость источника

При необходимости обеспечения неотказуемости источника структуры EDIFACT, это следует выполнять в соответствии с положениями ИСО/МЭК 10181-4 с использованием надлежащей пары групп сегментов заголовка и окончания защиты.

Служба защиты, обеспечивающая неотказуемость источника, должна быть определена в сегменте USH, алгоритм хеширования – в сегменте USA группы сегментов 1, а асимметричный алгоритм электронной подписи – в сегментах USA группы сегментов 2, при использовании сертификатов.

Если сертификат не передается в сообщении/пакете, асимметричный алгоритм должен быть обязательно известен получающей стороне. В этом случае асимметричный алгоритм должен быть определен в соглашении об обмене.

Сторона, действующая как инициатор защиты, должна вычислить цифровую подпись для передачи ее в сегменте USR группы сегментов окончания защиты. Сторона, действующая как адресат защиты, должна проверить значение цифровой подписи.

Рассмотренная служба должна обеспечить также целостность контента и аутентификацию источника.

5.3 Внутреннее представление информации и фильтры для обеспечения соответствия синтаксическим правилам EDIFACT

Использование математических алгоритмов для вычисления контрольных параметров целостности и цифровых подписей приводит к возникновению двух проблем.

Первая проблема заключается в том, что результат вычислений зависит от внутреннего представления набора знаков. При этом вычисление цифровой подписи отправителем и проверка ее подлинности получателем должны осуществляться с использованием одинакового способа кодирования набора знаков. Поэтому отправитель может указать то представление знаков, которое следует использовать для получения исходного значения контрольного параметра защиты.

Вторая проблема заключается в том, что результат вычислений представляет собой битовую конфигурацию, кажущуюся случайной. Это может привести к возникновению затруднений при передаче данных и работе интерпретирующих программ. Рекомендуется во избежание указанных затруднений обрабатываемую битовую конфигурацию предварительно подвергнуть обратному отображению на конкретное использованное представление набора знаков с помощью функции фильтрации. В целях упрощения этой процедуры следует использовать только одну функцию фильтрации для каждой службы защиты. Проблему появления аномальных терминальных знаков на выходе такого обратного отображения решается с помощью управляющей последовательности.

6 Правила использования групп сегментов заголовка и окончания защиты обмена и группы для пакетного ЭОД

6.1 Защита на уровнях групп и обменов (комплексная защита сообщений)

Угрозы безопасности, свойственные процессам передачи сообщений/пакетов, и связанные с ними службы защиты, описанные в приложениях А и В, сохраняются и на уровнях групп и обменов.

Методы защиты, рассмотренные в предыдущем разделе применительно к сообщениям/пакетам, могут также использоваться применительно к обменам и группам.

Для защиты на уровнях групп и обменов следует использовать те же группы сегментов заголовка и окончания защиты, что и на уровне сообщений/пакетов, а перекрестные ссылки между заголовком и окончанием должны всегда осуществляться на одном и том же уровне, даже если защита реализуется раздельно на нескольких уровнях.

Если защита применяется на уровне сообщения/пакета, защищаемой структурой является тело сообщения или объект. На уровне групп защищаемой структурой является набор сообщений/пакетов внутри группы, включая все заголовки и окончания сообщений/пакетов. На уровне обмена объектом защиты является совокупность сообщений/пакетов или групп в рамках обмена, включая все заголовки и окончания сообщений/пакетов или групп.

6.2 Группы сегментов заголовка и окончания защиты

На рисунке 5 приведена схема обмена, при которой обеспечена защита как на уровне обмена, так и на уровне групп.

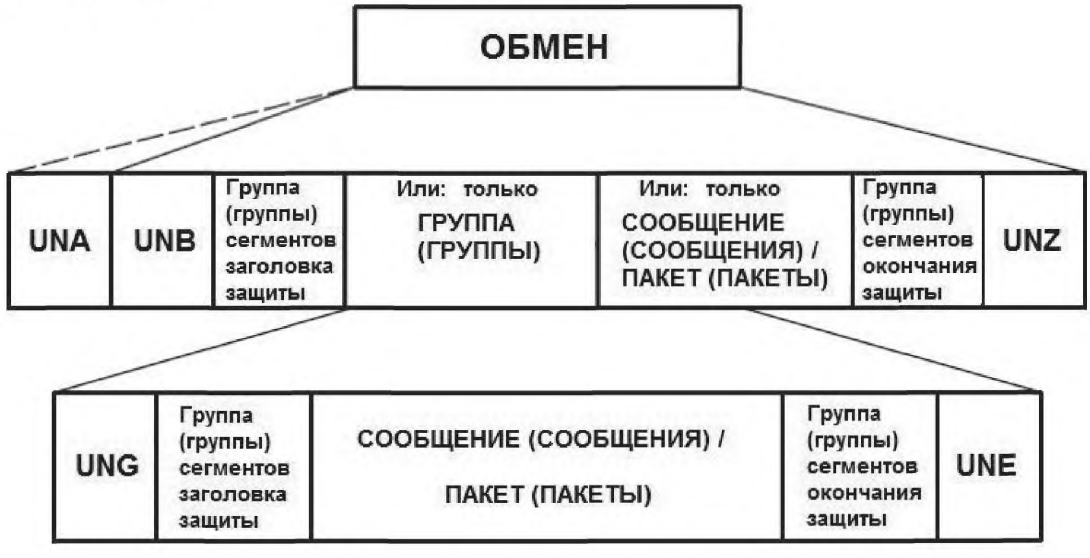

Рисунок 5 – Схематическое представление обмена, обеспечивающее защиту как на уровне обмена, так и на уровне групп

6.3 Структура, образуемая группами сегментов заголовка и окончания защиты

Таблица 3 – Группы сегментов заголовка и окончания защиты (безопасность только на уровне обмена)

ТЕГ	Наименование	S	R	
UNB	Заголовок обмена	M	1	
-----	Группа сегментов 1 ----------	C	99	--------+
USH	Заголовок защиты	M	1	I
USA	Алгоритм защиты	C	3	I
-----	Группа сегментов 2 ----------	C	2	----+ I
USC	Сертификат	M	1	I I
USA	Алгоритм защиты	C	3	I I
USR	Результат защиты	C	1	--------+
	Группа (группы) или сообщение (сообщения)/пакет (пакеты)			
-----	Группа сегментов n ----------	C	99	----+
UST	Окончание защиты	M	1	I
USR	Результат защиты	C	1	----+
UNZ	Окончание обмена	M	1	

Таблица 4 – Группы сегментов заголовка и окончания защиты (безопасность только на уровне группы)

ТЕГ	Наименование	S	R	
UNG	Заголовок группы	M	1	
-----	Группа сегментов 1 ----------	C	99	--------+
USH	Заголовок защиты	M	1	I
USA	Алгоритм защиты	C	3	I
-----	Группа сегментов 2 ----------	C	2	----+ I
USC	Сертификат	M	1	I I
USA	Алгоритм защиты	C	3	I I
USR	Результат защиты	C	1	--------+
	Сообщение (сообщения)/пакет (пакеты)			
-----	Группа сегментов n ----------	C	99	----+
UST	Окончание защиты	M	1	I
USR	Результат защиты	C	1	----+
UNE	Окончание группы	M	1	

Примечание – Полное описание спецификаций сегментов и элементов данных, включая сегменты заголовка обмена UNB, окончания обмена UNZ, заголовка группы UNG и окончания группы UNE приведено в ИСО 9735-10. В настоящем стандарте они не детализируются.

6.4 Область защиты

Допускается использовать два варианта применения области защиты:

1. Вычисление каждого из значений параметров целостности и аутентификации данных, а также формирование цифровых подписей начинается с прямой обработки текущей группы сегментов заголовка защиты и группы (групп) или сообщения(ий) / пакета(ов). В этом случае область защитыне должна охватывать никакие другие группы сегментов заголовка защитыили окончания защиты.

Отсчет знаков группы сегментов заголовка защиты следует начинать с первого знака (с буквы “U”) и заканчивать разделителем включительно, следующим за этой группой сегментов, а группа(группы) или сообщение(ия) /пакет(пакеты) – с первого знака после разделителя,

завершающего последнюю группу сегментов заголовка защиты, до разделителя, предшествующего первому знаку первой группы сегментов окончания защиты включительно.

Таким образом, порядок, в котором осуществляются службы защиты, заранее не регламентируется, и они являются полностью независимыми друг от друга.

Рисунки 6 и 7 иллюстрируют этот случай (область применения службы защиты, определенная в заголовке защиты 2, выделена темно-серым цветом).

UNB	Группа 3 сегментов заголовка защиты	Группа 2 сегментов заголовка защиты	Группа 1 сегментов заголовка защиты	ГРУППА (ГРУППЫ) ИЛИ СООБЩЕНИЕ (СООБЩЕНИЯ)/ ПАКЕТ (ПАКЕТЫ)	Группа 1 сегментов окончанияз ащиты	Группа 2 сегментов окончания защиты	Группа 3 сегментов окончания защиты	UNZ

Рисунок 6 – Схематическое представление области защиты: только группа сегментов заголовка защиты и группа (группы) или сообщение(ия) / пакет (пакеты)

UNG	Группа 3 сегментов заголовка защиты	Группа 2 сегментовзаголовка защиты	Группа 1 сегментов заголовка защиты	СООБЩЕНИЕ (СООБЩЕНИЯ)/ПАКЕТ (ПАКЕТЫ)	Группа 1 сегментов окончания защиты	Группа 2 сегментовокончанияащиты	Группа 3 сегментовокончанияащиты	UNE

Рисунок 7 – Схематическое представление области защиты: только группа сегментов заголовка защиты и сообщение(ия) / пакет (пакеты)

2. Вычисления начинают с текущей группы сегментов заголовка защиты и заканчивают связанной с ней группой сегментов окончания защиты, включительно. В этом случае область защиты должна охватывать текущую группу сегментов заголовка защиты, группу (группы) или сообщение(ия) /пакет (пакеты), а также все остальные вложенные группы сегментов заголовка и окончания защиты.

Эта область должна включать в себя каждый знак – от первой буквы “U” текущей группы сегментов заголовка защиты до разделителя, предшествующего первому знаку соответствующей группы сегментов окончания защиты, включительно.

Иллюстрация данного случая приведена на рисунках 8 и 9, где область применения службы защиты, определенная в заголовке защиты 2, выделена темно-серым цветом.

UNB	Группа 3 сегментов заголовка защиты	Группа 2 сегментов заголовка защиты	Группа 1 сегментов заголовка защиты	ГРУППА (ГРУППЫ) ИЛИ СООБЩЕНИЕ (СООБЩЕНИЯ)/ПАКЕТ (ПАКЕТЫ)	Группа 1 сегментов окончанияза щиты	Группа 2 сегментов окончанияза щиты	Группа 3 сегментов окончанияз ащиты	UNZ

Рисунок 8 – Схематическое представление области защиты (от группы сегментов заголовка защиты до группы сегментов окончания защиты)

UNG	Группа 3 сегментов заголовка защиты	Группа 2 сегментов заголовка защиты	Группа 1 сегментов заголовка защиты	СООБЩЕНИЕ (СООБЩЕНИЯ)/ПАКЕТ(Ы)	Группа 1 сегментов окончанияз ащиты	Группа 2 сегментов окончанияз ащиты	Группа 3 сегментов окончанияз ащиты	UNE

Рисунок 9 – Схематическое представление области защиты (от группы сегментов заголовка защиты до группы сегментов окончания защиты)

Для каждой добавляемой службе защиты допускается применять любой из вышеуказанных подходов.

В обоих случаях связь между группой сегментов заголовка защиты и соответствующей группой сегментов окончания защиты должна обеспечиваться элементами данных «справочный номер защиты» в сегментах USH и UST.

Приложение А
(справочное)
Угрозы безопасности EDIFACT и технические решения проблемы

А.1 Введение

В данном приложении описаны типичные угрозы безопасности, свойственные процессам передачи сообщений/пакетов между отправителями и получателями, а также общие методы противодействия этим угрозам. Угрозы безопасности и технические решения по их преодолению имеют отношение к любому уровню: сообщений/пакетов групп или обменов.

А.2 Угрозы безопасности

Хранение и передача сообщений/пакетов EDIFACT в электронной среде подвержены целому ряду угроз, к числу которых относятся:

- несанкционированное раскрытие информации, содержащейся в сообщениях и пакетах;
- умышленное внедрение посторонних сообщений/пакетов;
- копирование, утеря или воспроизведение сообщений/пакетов;
- внесение изменений в содержимое сообщения/пакета;
- уничтожение сообщений/пакетов;
- отрицание отправителем или получателем сообщения/пакета факта его передачи или приема.

Все эти угрозы могут быть результатом умышленных действий (как, например, незаконное манипулирование содержимым сообщения/пакета) или случайной ошибки при передаче данных, которая приводит к изменению содержимого (контента) сообщения/пакета.

А.3 Защитные решения — основные службы и принципы их использования

А.3.1 Общие положения

Для противодействия перечисленным в А.2 угрозам разработан целый ряд механизмов защиты, в которых использованы те или иные методы достижения определенных целей.

Прежде всего, важно однозначно идентифицировать взаимодействующие стороны, вовлеченные в обеспечение защиты сообщений/пакетов: инициатора защиты (далее – отправитель), который перед передачей сообщения/пакета осуществляет его защиту, и адресата защиты (далее – получатель), который выполняет проверку полученного сообщения/пакета. Эти стороны могут быть идентифицированы в сегментах защиты. При применении асимметричных алгоритмов защиты такая идентификация может быть реализована путем использования так называемых «сертификатов» (в действительности это может быть либо сам сертификат, либо его учетный номер), описание которых приведено ниже.

Как правило, в открытой системе требуется обращение к органу сертификации. Это третья сторона процесса информационного обмена, которой в определенной степени доверяют вовлеченные в обмен стороны и которая необходима для идентификации и регистрации всех пользователей с открытыми ключами. Эта информация передается другим пользователям с помощью сертификата, который представляет собой цифровую подпись, «поставленную» органом сертификации на сообщении, состоящем из идентификатора пользователя и его открытого ключа. В такой ситуации принцип доверия реализуется чисто функциональным способом и не требует применения секретных или закрытых ключей.

Альтернативный подход к обеспечению безопасности заключается в использовании симметричных методов защиты для установления подлинности взаимодействующих сторон, которые должны быть указаны в полях имен отправителя и получателя в системе защиты.

Сообщение/пакет может быть обеспечен защитой одновременно несколькими сторонами (например, может снабжаться несколькими цифровыми подписями), благодаря чему относящаяся к защите информация может повторяться, позволяя тем самым идентифицировать несколько подписывающих или проверяющих сторон, и, соответственно, включать в себя несколько цифровых подписей или контрольных значений.

Требования и методы, предназначенные для защиты сообщений/пакетов, групп или обменов EDIFACT, приведены ниже.

А.3.2 Целостность цепочки

Целостность цепочки обеспечивает защиту от копирования, дополнения, изъятия, потери или воспроизведения структуры EDIFACT (сообщения/пакета, группы или обмена).

Для обнаружения потери сообщений/пакетов, групп или обменов:

- отправитель может включить, а получатель проверить порядковый номер (относящийся к потоку сообщений/пакетов между двумя участвующими сторонами);
- отправитель может запросить подтверждение приема (квитирование) и проверить его правильность.

Для обнаружения добавленных или дублированных сообщений/пакетов, групп или обменов:

- отправитель может включить, а получатель проверить порядковый номер;
- отправитель может включить, а получатель проверить отметку времени.

В случае использования порядковых номеров стороны должны согласовать между собой правила манипулирования такими номерами.

Обычно отметка времени должна создаваться системой отправителя. Это означает, что исходную точность отметки времени определяет отправитель.

Для обеспечения полной защиты целостность отметки времени или порядкового номера должна быть обеспечена одной из функций, рассмотренных ниже.

А.3.3 Целостность информационного содержимого

Целостность информационного содержимого (контента) обеспечивает защиту от внесения изменений в данные.

Защита может быть обеспечена отправителем посредством введения контрольного параметра целостности. Значение этого параметра вычисляют с помощью надлежащего криптографического алгоритма, в частности такого, как MDC [ModificationDetectionCode (код для обнаружения изменений)]. Так как это контрольное значение само по себе не защищено, к нему должны применяться дополнительные меры защиты, такие как пересылка контрольного значения по отдельному каналу или вычисление цифровой подписи с целью получения гарантии неотказуемости источника. Как вариант, на целостность содержимого может влиять аутентификация отправителя, выполняемая с использованием кода аутентификации сообщения. В этом случае получатель с помощью соответствующих алгоритмов и параметров вычисляет контрольное значение параметра целостности реально принятых данных и сравнивает результат вычисления с полученным контрольным значением.

В рамках ЭОД обеспечение целостности содержимого обычно является производным результатом аутентификации источника или неотказуемости источника.

А.3.4 Аутентификация источника

Аутентификация источника защищает получателя от того, что реальным отправителем сообщения/пакета, группы или обмена окажется иная (авторизованная) сторона, отличающаяся от заявленной.

Защита обеспечивается путем вставки контрольного значения параметра аутентификации, например кода аутентификации сообщения (MAC). Значение этого параметра зависит как от информационного содержимого, так и от секретного ключа, принадлежащего отправителю.

Служба аутентификации источника может включать в себя службу обеспечения целостности контента и быть производным результатом службы неотказуемости источника.

В большинстве случаев рекомендуется иметь хотя бы службу аутентификации источника.

А.3.5 Неотказуемость источника

Неотказуемость источника защищает получателя сообщения/пакета, группы или обмена от отказа отправителя от факта посылки этих структур.

Защита может обеспечиваться путем включения цифровой подписи отправителя (а также путем реализации соответствующей процедуры «аутентификации источника», основанной на использовании защищенных от внешних воздействий аппаратных средств, или путем привлечения доверенных третьих сторон). Цифровая подпись формируется на основе шифрования с помощью асимметричного алгоритма и закрытого ключа некоторого объекта либо контрольного значения, извлеченного из передаваемых данных (например, с использованием хеш-функции).

Цифровая подпись может быть проверена на подлинность с помощью открытого ключа, который соответствует закрытому ключу, примененному при ее создании. Открытый ключ может быть указан в соглашении об обмене, которое подписано партнерами, или может быть указан в сертификате с цифровой подписью органа сертификации. Сертификат может пересылаться в составе структуры EDIFACT.

Цифровая подпись не только гарантирует неотказуемость источника, но и обеспечивает целостность контента и аутентификацию источника.

А.3.6 Неотказуемость приема

Неотказуемость приема защищает отправителя сообщения/пакета, группы или обмена от непризнания факта их получения адресатом.

Защита может обеспечиваться путем обязательного квитирования принятого сообщения получателем и посылки квитанции, которая содержит цифровую подпись, сформированную на основе данных исходной структуры EDIFACT. Квитанция имеет форму служебного сообщения, пересылаемого получателем отправителю.

А.3.7 Конфиденциальность содержимого

Конфиденциальность содержимого предотвращает возможность несанкционированного прочтения, копирования или разглашения содержимого сообщения/пакета, группы или обмена.

Защита может обеспечиваться путем шифрования данных с использованием симметричного алгоритма с секретным ключом, общим для отправителя и получателя.

Однако секретный ключ может быть передан тайно после его шифрования по асимметричному алгоритму с использованием открытого ключа получателя.

Требования к службе конфиденциальности установлены в ИСО 9735-7.

А.3.8 Взаимосвязь служб защиты

Некоторые из служб изначально включают в себя иные службы, благодаря чему исчезает необходимость добавления служб, которые реализуются неявным образом. Например, использование механизма, обеспечивающего неотказуемость источника, неявно приводит к сохранению целостности контента. Взаимосвязи служб приведены в таблице А.1.

Таблица А.1 — Взаимосвязь служб

Служба защиты	влечет за собой также обеспечение		
	целостности содержимого	аутентификации источника	неотказуемости источника
Целостность содержимого	Да	—	—
Аутентификация источника	Да	Да	—
Неотказуемость источника	Да	Да	Да

Приложение В
(справочное)
Способы защиты структуры EDIFACT

В.1 Общие положения

В данном приложении описаны некоторые из основополагающих этапов обеспечения безопасности структур EDIFACT: сообщений/пакетов, групп и обменов. Подробное описание и объяснение принципов защиты приведено в приложении А настоящего стандарта, а также в ИСО 7498-2, ИСО/МЭК 9594-8 и в документе CCITT X.509.

На первом этапе определяют (совместно с партнерами) реальные потребности в службах защиты. Службы защиты, доступные в среде EDIFACT, указаны ниже, и из необходимо выбрать те, которые способны предотвратить выявленные угрозы деятельности конкретного предприятия или организации. Обычно эти потребности могут быть выявлены по результатам аудита, как внутреннего, так и внешнего. Базовыми службами защиты, доступными на стороне отправителя, являются следующие:

- целостность содержимого,
- аутентификация источника и
- неотказуемость источника.

Эти службы не являются независимыми, потому нет необходимости в использовании дополнительных служб, которые реализуются неявным образом. Например, использование службы неотказуемости источника неявно влечет за собой и сохранение целостности контента.

Такие взаимосвязи указаны в таблице А.1 приложения А. С учетом приведенных в ней взаимосвязей отправитель должен выбрать не более одной из трех указанных служб.

Неотказуемость приема – это служба, которая должна быть инициирована получателем. Она может быть запрошена отправителем явным образом или может быть определена как обязательная в соглашении об обмене. Для передачи такого запроса используют стандартное сообщение AUTACK.

В.2 Двустороннее соглашение об обмене или привлечение третьей стороны

Если службы защиты должны быть интегрированы, то партнеры должны заключить дополнительные соглашения. Возможен ряд подходов к решению этого вопроса. Краткое описывание двух из них, которые считают экстремальными, приведено ниже.

Минимальным требованием должно быть заключение с каждым из партнеров отдельного двустороннего соглашения об использовании служб защиты, конкретных алгоритмов, кодов, методов управления ключами, действий в случае ненадлежащего поведения и т. п. Образец подобного соглашения доступен в рамках программы TEDIS Европейской комиссии. При таком подходе в сообщение/пакет должен быть включен небольшой объем информации, касающейся обеспечения защиты.

Другой экстремальный подход заключается в том, чтобы привлечь третью сторону, выступающую в роли органа сертификации, который регистрирует всех пользователей и выдает сертификаты на пользовательские открытые ключи. В данном случае адекватным решением может быть заключение соглашения с сертификационным органом, который при этом, как правило, должен отвечать также за ведение «черных списков». Данный подход может потребовать включения в сообщение/пакет гораздо большего объема информации, касающейся обеспечения защиты.

Службы защиты интегрируются в структуры EDIFACT таким образом, чтобы обеспечивалась максимальная гибкость и поддерживались оба подхода, описанных выше.

В.3 Практические аспекты

Для эффективной реализации служб защиты необходимо учитывать множество различных аспектов, таких как: генерация ключей; потребность в трансляторе, способном обрабатывать сегменты защиты; внутренние процедуры поддержки полномасштабного использования служб защиты (например, организация хранения входящих сообщений/пакетов с цифровыми подписями, манипулирование множественными цифровыми подписями) и т. п.

Следует подчеркнуть, что интеграция служб защиты должна быть абсолютно прозрачной для используемых протоколов передачи данных и не зависит от них. Если конкретная система обеспечивает передачу обычных сообщений/пакетов EDIFACT, это означает, что она будет также способна передавать защищенные сообщения/пакеты этого типа.

В.4 Процедура конструирования защищенной структуры EDIFACT

После создания сообщения/пакета, группы или обмена структуры EDIFACT определяют и реализуют необходимые службы защиты. Если службы защиты основаны на использовании цифровых подписей, то для ее обеспечения непосредственно или косвенно должны быть привлечены

лица, имеющие закрытые ключи. Делать это сразу после создания структуры EDIFACT не обязательно.

Аналогично этому, для входящих структур EDIFACT, первым шагом должна быть проверка параметров служб защиты и сохранение защищенных структур EDIFACT для контроля и документирования.

B.5 Последовательность применения служб защиты

Порядок, в котором используются службы защиты, целиком определяет пользователь, так как службы могут быть независимыми друг от друга. В частности, в случае применения множественных цифровых подписей без встраивания групп сегментов заголовка и окончания защиты, последовательность, в которой они вычисляются и проверяются, не имеет значения.

B.6 Защита отдельным сообщением на уровне сообщений/пакетов

B.6.1 Требования бизнеса

Существуют два следующих требования бизнеса к данной функциональной возможности:

a) обеспечить защиту одного или нескольких сообщений/пакетов единственным отдельным сообщением отправителя,

b) обеспечить гарантированное подтверждение отправителю факта получения одного или нескольких исходных сообщений/пакетов без их возврата.

Эти требования могут быть выполнены путем использования сообщения для защищенной аутентификации и защищенного квитирования AUTACK, подробно описанного в ИСО 9735-6.

B.6.2 Защита отдельным сообщением, используемая отправителем

Такое использование сообщения AUTACK позволяет отправителю предоставить любую службу защиты путем передачи ее параметров в отдельном сообщении. Таким образом службы защиты могут подключаться на более позднем или более подходящем этапе. Кроме этого они могут обеспечивать защиту нескольких исходных сообщений/пакетов, в отличие от прямого встраивания функций защиты на уровне сообщения/пакета, которое обеспечивает защиту только одного сообщения/пакета за одну передачу.

Принципы использования защиты идентичны для интеграционного и раздельного подходов, но для последнего необходимо наличие уникальной ссылки на защищаемую исходную структуру «сообщение/пакет».

B.6.3 Защита отдельным сообщением, используемая получателем

Такое использование сообщения AUTACK ориентировано на обеспечение неотказуемости приема. Подробное описание сообщения AUTACK приведено в ИСО 9735-6.

Сообщение AUTACK может использоваться как защищенное подтверждение приема (квитирование), пересылаемое получателем одного или нескольких обменов либо одного или нескольких сообщений/пакетов в одном или нескольких сеансах обмена их отправителю. Критерии и средства, с помощью которых формируется сообщение AUTACK, гарантированно предоставляют отправителю одного либо нескольких сообщений/пакетов или обменов защищенное уведомление о том, что они были получены нужным адресатом.

B.7 Защита отдельным сообщением на уровнях групп или обменов

Метод, описанный в разделе B.6 может быть использован также для защиты полных групп или полных обменов.

Существуют два требования бизнеса к данной функциональной возможности:

a) обеспечить защиту одной или нескольких групп либо одного или нескольких обменов в единственном отдельном сообщении отправителя,

b) обеспечить гарантированное подтверждение отправителю факта получения исходных групп или обменов без их возврата.

Эти требования могут быть выполнены путем использования сообщения защищенной аутентификации и защищенного квитирования AUTACK, подробно описанного в ИСО 9735-6.

Приложение С
(справочное)
Примеры защиты сообщений

С.1 Введение

В данном приложении приведены три примера применений служебных сегментов защиты.

Все примеры основаны на использовании платежных поручений EDIFACT из справочника финансовых сообщений MIG, опубликованного в рамках Международной межбанковской системы передачи информации и совершения платежей (SWIFT). Однако описанные ниже механизмы защиты не зависят от типа сообщения и могут использоваться применительно к любому сообщению EDIFACT.

Пример 1. Аутентификация источника сообщения

Данный пример показывает, каким образом служебные сегменты защиты могут использоваться в случае применения **симметричного алгоритма** защиты для обеспечения аутентификации источника сообщения. В этом случае происходит предварительный обмен симметричным ключом между партнерами, потому группа сегментов заголовка защиты содержит всего два довольно простых сегмента.

Пример 2. Неотказуемость источника (первый метод)

Данный пример показывает, как служебные сегменты защиты могут использоваться в случае применения **асимметричного алгоритма** защиты для обеспечения неотказуемости источника. Алгоритмом, применяемым непосредственно к передаваемому сообщению является **функция хеширования,** которая не требует предварительного обмена ключами между партнерами. Значение хеш-функции подписывается с использованием ассиметричного алгоритма. Открытый ключ, необходимый получателю для проверки подписи в сообщении, включают в сегмент сертификата, который передается в группе сегментов заголовка защиты сообщения. Этот сертификат должен быть подписан его издателем («органом сертификации») и должен содержать открытый ключ органа сертификации для предоставления любому из партнеров возможности проверить целостность и подлинность сертификата.

Пример 3. Неотказуемость источника (второй метод)

Данный пример показывает, как служебные сегменты защиты могут использоваться в случае применения **асимметричного алгоритма** защиты для обеспечения неотказуемости источника. В данном случае непосредственно к сообщению применяют **симметричный алгоритм**, который требует предварительного обмена симметричным ключом между партнерами и предоставляет контрольное значение параметра целостности. Указанный симметричный ключ должен быть передан в составе группы сегментов заголовка защиты сообщения и зашифрован с применением асимметричного алгоритма с использованием открытого ключа ожидаемого получателя.

Контрольное значение параметра целостности подписывается с помощью асимметричного алгоритма. Открытый ключ, необходимый получателю для проверки подписи в сообщении, включают в первый сегмент сертификата, который передается в группе сегментов заголовка защиты сообщения. Этот сертификат должен быть подписан его издателем (органом сертификации) и должен содержать открытый ключ органа сертификации для предоставления любому из партнеров возможности проверить целостность и подлинность сертификата.

Второй сегмент сертификата содержит ссылку на открытый ключ ожидаемого получателя, использованный отправителем сообщения для защиты симметричного ключа.

Данный метод используют банки Франции в рамках системы ETEBAC 5 (защищенная система передачи файлов между банками и корпоративными клиентами).

В двух последних примерах любой из партнеров, доверяющий органу сертификации, имеет возможность проверить подлинность подписи в полученном сообщении, пользуясь только данными, содержащимися в сообщении.

С.2 Пример 1. Аутентификация источника сообщения

С.2.1 Краткое описание

Компания А поручает Банку А (код 603000) списать с ее счета №00387806 сумму 54345,10 фунтов стерлингов 9 апреля 1996 г. Эта сумма должна быть переведена в Банк В (код 201827) на счет № 00663151 Компании В, находящейся по адресу WestDock, MilfordHaven. Платеж производится на основании выставленного счета № 62345. Контактное лицо получателя платежа – м-р Джонс, отдел продаж.

Банк А требует, чтобы платежное поручение было защищено функцией защиты «аутентификация источника сообщения», которая осуществляется путем генерирования отправителем сообщения так называемого «кода аутентификации сообщения» (MAC) с помощью

симметричного алгоритма шифрования “DataEncryptionStandard” (DES) в соответствии с требованиями ИСО 8731-1; этот код подлежит проверке Банком А. Предполагается, что предварительно состоялся обмен секретным DES-ключом между Компанией А и Банком А.

Примечание – Далее рассмотрены только части сообщения, имеющие отношение к обеспечению защиты.

С.2.2 Элементы защиты

ЗАГОЛОВОК ЗАЩИТЫ	
СЛУЖБА ЗАЩИТЫ	Аутентификация источника сообщения
КОНТРОЛЬНЫЙ НОМЕР СЛУЖБЫ ЗАЩИТЫ	Данный заголовок имеет контрольный номер 1
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения MAC фильтруются с помощью шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	При формировании MAC сообщение закодировано с помощью набора 8-битовых знаков ASCII
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Отправитель сообщения (сторона, формирующая код аутентификации сообщения - MAC).	М-р СМИТ из Компании А
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Получатель сообщения (сторона, которая проверяет код аутентификации сообщения - MAC).	Банк А
ПОРЯДКОВЫЙ НОМЕР ЗАЩИТЫ	Порядковый номер защиты данного сообщения 001
ДАТА И ВРЕМЯ ЗАЩИТЫ	Защитная отметка времени: дата: 1996 04 09[1)], время: 13:59:50
АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется симметричный алгоритм для аутентификации источника сообщения. MAC вычисляется в соответствии с требованиями ИСО 8731-1 Используют алгоритм DES
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Идентифицирует указанное ниже значение параметра алгоритма как имя предварительно переданного симметричного ключа Используется ключ с именем MAC-KEY1
ОКОНЧАНИЕ ЗАЩИТЫ	
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Данное окончание имеет контрольный номер 1
ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	4
РЕЗУЛЬТАТ ЗАЩИТЫ	
РЕЗУЛЬТАТ ПРОВЕРКИ ПОДЛИННОСТИ Квалификатор контрольного значения Контрольное значение	 MAC Четырехбайтовый результат проверки подлинности (код аутентификации сообщения)

[1)] Представление даты соответствует оригиналу.

С.3 Пример 2. Неотказуемость источника (первый метод)

С.3.1 Краткое описание

Банку А необходима служба защиты «неотказуемость источника»для платежного поручения Компании А, переданного м-ром Смитом.

В соглашении об обмене между сторонами установлено, что необходимая Банку А служба защиты «неотказуемость источника» для платежных поручений, пересылаемых мистером Смитом из компании А, осуществляется с использованием одной цифровой подписи.

Сертификат, удостоверяющий открытый ключ м-ра Смита, выдан органом, которому доверяют обе стороны – эмитентом сертификата.

С.3.2 Элементы защиты

ЗАГОЛОВОК ЗАЩИТЫ	
СЛУЖБА ЗАЩИТЫ	Неотказуемость источника
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Данный заголовок имеет контрольный номер 1
ТИП ОТВЕТА	Подтверждение не требуется
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения (подписи) фильтруются с помощью шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	При формировании подписи сообщение было закодировано с помощью набора 8-битовых знаков ASCII
ПОРЯДКОВЫЙ НОМЕР ЗАЩИТЫ	Порядковый номер защиты данного сообщения 202
ДАТА И ВРЕМЯ ЗАЩИТЫ	Защитная отметка времени: дата: 1996 01 15[1)], время: 10:05:30
АЛГОРИТМ ЗАЩИТЫ	Хеш-функция, используемая м-ром СМИТОМ для формирования подписи
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм хеширования владельца сертификата. Хеш-функция, соответствующая ИСО/МЭК 10118-2, в которой применяется *n*- битовый блочный алгоритм шифрования для получения хеш-кода двойной длины (128 битов); начальные значения: IV = 0F 0F0F0F0F0F0F0F IV' = F0 F0F0F0F0F0F0F0; правила дополнения незначащими битами – как определено в первом варианте п. В.3 стандарта ИСО/МЭК 10118-2:2000; преобразования u и u' – согласно приложению А ИСО/МЭК 10118-2:2000. Используется блочный алгоритм шифрования DES
СЕРТИФИКАТ	Сертификат м-ра СМИТА
УЧЕТНЫЙ НОМЕР СЕРТИФИКАТА	Данный сертификат выдан сертификационным органом AUTHORITY и имеет учетный номер 00000001
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны защиты	 Владелец сертификата: м-р СМИТ из Компании А
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны защиты Имя ключа	 Удостоверяющая сторона: сертификат м-ра СМИТА выдан органом сертификации AUTHORITY. Открытый ключ AUTHORITY, использованный для создания сертификата м-ра СМИТА, имеет имя PK1

[1)] Представление даты соответствует оригиналу.

СИНТАКСИС И ВЕРСИЯ СЕРТИФИКАТА	Версия сертификата указывается в справочнике служебных сегментов UN/EDIFACT
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения (ключи и цифровые подписи) фильтруются с помощью шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	Удостоверение сертификата закодировано с помощью набора 8-битовых знаков ASCII при изготовлении сертификата
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является терминатор сегмента. Значение « ' » (апостроф).
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является разделитель элементов данных. Значение «+» (знак плюс)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является разделитель компонентных элементов данных. Значение «:» (двоеточие)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является разделитель повторов. Значение «*» (звездочка)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является знак освобождения. Значение «?» (знак вопроса)
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Время создания сертификата Сертификат м-ра СМИТА изготовлен 931215[1)] в 14:12:00
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Начало срока действия сертификата Начало срока действия сертификата м-ра СМИТА 1996 01 01 000000[2)]
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Окончание срока действия сертификата Окончание срока действия сертификата м-ра СМИТА 1996 12 31 235959 [3)]
АЛГОРИТМ ЗАЩИТЫ	Асимметричный алгоритм, используемый м-ром СМИТОМ для подписи
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм подписи владельца сертификата. Ни один из режимов здесь не применим. Асимметричный алгоритм RSA
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как открытую экспоненту для проверки подлинности подписи. Открытый ключ м-ра СМИТА

[1)] Представление даты соответствует оригиналу.
[2)] Представление даты и времени соответствует оригиналу.
[3)] Представление даты и времени соответствует оригиналу.

ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как модуль для проверки подлинности подписи. Модуль м-ра СМИТА
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как длину модуля м-ра СМИТА (в битах). Длина модуля м-ра СМИТА 512 битов
АЛГОРИТМ ЗАЩИТЫ	Хеш-функция, используемая органом сертификации AUTHORITY для изготовления сертификата м-ра СМИТА
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм хеширования издателя сертификата. Хеш-функция, соответствующая ИСО/МЭК 10118-2, в которой применяется *n*- битовый блочный алгоритм шифрования для получения хеш-кода двойной длины (128 битов); начальные значения: IV = 0F 0F0F0F0F0F0F0F IV' = F0 F0F0F0F0F0F0F0; правила дополнения незначащими битами –согласно первому варианту приложения B, раздел B.3 ИСО/МЭК 10118-2:2000; преобразования u и u' – согласно приложению A ИСО/МЭК 10118 -2:2000. Используется блочный алгоритм шифрования DES
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм цифровой подписи издателя сертификата. Ни один из режимов не применим. Асимметричный алгоритм RSA
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как открытую экспоненту для проверки подлинности подписи. Открытый ключ органа сертификации AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как модуль для проверки подлинности подписи. Модуль органа сертификации AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как длину модуля органа сертификации AUTHORITY (в битах). Длина модуля органа сертификации AUTHORITY: 512 битов
РЕЗУЛЬТАТ ЗАЩИТЫ	Цифровая подпись сертификата
РЕЗУЛЬТАТ ПРОВЕРКИ ПОДЛИННОСТИ Квалификатор контрольного значения Контрольное значение.	 Уникальное контрольное значение: 1. 512-битовая цифровая подпись
ОКОНЧАНИЕ ЗАЩИТЫ	
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Окончание защиты имеет контрольный номер 1
ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	9
РЕЗУЛЬТАТ ЗАЩИТЫ	Цифровая подпись сообщения
РЕЗУЛЬТАТ ПРОВЕРКИ ПОДЛИННОСТИ Квалификатор контрольного значения. Контрольное значение.	 Уникальное контрольное значение:1. 512-битовая цифровая подпись.

С.4 Пример 3: неотказуемость источника (второй метод)

С.4.1 Краткое описание

Банку А необходима служба защиты «неотказуемость источника» для платежного поручения Компании А, переданного м-ром Смитом. Компания А запрашивает защищенное квитирование от Банка А (неотказуемость приема), которое должно быть передано в сообщении AUTACK.

В соглашении об обмене между сторонами установлено, что служба защиты «неотказуемость источника» для платежных поручений, выдаваемых мистером Смитом из компании А, осуществляется с использованием одной цифровой подписи.

По согласию обеих сторон, для вычисления этой цифровой подписи используется ассимметричный алгоритм RSA с 512-битовым ключом, который применяется к 64-битовому значению параметра целостности, рассчитанному с помощью симметричного алгоритма DES в режиме CBC. Сертификат, удостоверяющий открытый ключ м-ра Смита, выдан органом, которому доверяют обе стороны.

С.4.2 Элементы защиты

ЗАГОЛОВОК ЗАЩИТЫ	
СЛУЖБА ЗАЩИТЫ	Неотказуемость источника
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Данный заголовок имеет контрольный номер 1
ТИП ОТВЕТА	Требуется квитирование
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения фильтруются с использованием шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	При генерации подписи сообщение было закодировано с помощью набора 8-битовых знаков ASCII
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны защиты	Отправитель сообщения (сторона, защищающая сообщение): м-р Смит из Компании А
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны защиты	Получатель сообщения (сторона, проверяющая защиту сообщения): Банк А
ПОРЯДКОВЫЙ НОМЕР ЗАЩИТЫ	Порядковый номер защиты сообщения 001
ДАТА И ВРЕМЯ ЗАЩИТЫ	Защитная отметка времени: дата: 1996 01 15 [1], время: 10:05:30
АЛГОРИТМ ЗАЩИТЫ	Симметричный алгоритм, используемый для вычисления параметра целостности
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	Используется алгоритм хеширования владельца сертификата. Сцепление блоков шифротекста [2] по ИСО/МЭК 10116 (*n*-битовые блоки). Вычисляется 64-битовый параметр целостности; начальное значение – двоичный ноль; используется секретный ключ алгоритма DES; ключ передается зашифрованным с помощью открытого ключа Банка А. Используется блочный алгоритм шифрования DES
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	Определяет указанное ниже значение параметра алгоритма как симметричный ключ, зашифрованный открытым ключом. Симметричный ключ, зашифрованный открытым ключом Банка А

[1] Представление даты соответствует оригиналу.

[2] Соответствует английскому Cipher Block Chaining (CBC).

ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет указанное ниже значение параметра алгоритма как начальное значение, представленное открытым текстом. Начальное значение, представленное открытым текстом (все биты – двоичные нули)
СЕРТИФИКАТ	Сертификат м-ра СМИТА (отправителя сообщения)
УЧЕТНЫЙ НОМЕР СЕРТИФИКАТА	Данный сертификат имеет учетный номер 00000001, присвоенный органом AUTHORITY
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны защиты	 Владелец сертификата: м-р СМИТ из Компании А
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны защиты Имя ключа	 Проверяющая сторона: сертификат м-ра СМИТА был изготовлен органом сертификации AUTHORITY. PK1 – открытый ключ органа сертификации AUTHORITY, который был использован для изготовления сертификата м-ра Смита
СИНТАКСИС И ВЕРСИЯ СЕРТИФИКАТА	Версия сертификата по справочнику служебных сегментов UN/EDIFACT
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения (ключи и цифровые подписи) фильтруются с помощью шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	Удостоверение сертификата закодировано с помощью набора 8-битовых знаков ASCII при изготовлении сертификата
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является терминатор сегмента. Значение «'» (апостроф)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является разделитель элементов данных. Значение «+» (знак плюс)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является разделитель компонентных элементов данных. Значение «:» (двоеточие)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является разделитель повторов. Значение «*» (звездочка)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, используемый при вычислении подписи. Служебным знаком является знак освобождения. Значение «?» (знак вопроса)
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Время создания сертификата Сертификат м-ра СМИТА изготовлен 931215 [1] в 14:12:00

[1] Представление даты соответствует оригиналу.

ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Начало срока действия сертификата Начало срока действия сертификата м-ра СМИТА: 1996 01 01 000000[2)]
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Окончание срока действия сертификата Окончание срока действия сертификата м-ра СМИТА: 1996 12 31 235959 [3)]
АЛГОРИТМ ЗАЩИТЫ	Асимметричный алгоритм, используемый м-ром СМИТОМ для подписи
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм подписи владельца сертификата. Ни один режим не применим. Асимметричный алгоритм RSA
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как открытую экспоненту для проверки подлинности подписи. Открытый ключ м-ра СМИТА
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как модуль для проверки подлинности подписи. Модуль м-ра СМИТА
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как длину модуля м-ра СМИТА (в битах). Длина модуля м-ра СМИТА 512 битов
АЛГОРИТМ ЗАЩИТЫ	Хеш-функция, используемая органом сертификации AUTHORITY для изготовления сертификата м-ра СМИТА
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм хеширования издателя сертификата. Хеш-функция – Square-mod-n для RSA – по приложению D к документу CCITT X509.ИСО/МЭК 9594-8 Асимметричный алгоритм RSA
АЛГОРИТМ ЗАЩИТЫ	Асимметричный алгоритм, используемый органом сертификации AUTHORITY для подписи
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм подписи издателя. Ни один режим не применим. Асимметричный алгоритм RSA
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр в качестве открытой экспоненты для проверки подлинности подписи. Открытый ключ AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как модуль для проверки подлинности подписи. Модуль органа сертификации AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет параметр как длину модуля органа сертификации AUTHORITY (в битах). Длина модуля органа сертификации AUTHORITY 512 битов
РЕЗУЛЬТАТ ЗАЩИТЫ	Цифровая подпись сертификата

[2)] Представление даты и времени соответствует оригиналу.
[3)] Представление даты и времени соответствует оригиналу.

РЕЗУЛЬТАТ ПРОВЕРКИ ПОДЛИННОСТИ Квалификатор контрольного значения Контрольное значение	 Уникальное контрольное значение:1. 512-битовая цифровая подпись
СЕРТИФИКАТ	Сертификат Банка А (получателя сообщения).
УЧЕТНЫЙ НОМЕР СЕРТИФИКАТА	Открытый ключ Банка А ассоциируется с сертификатом, имеющим учетный номер 00001001
ОКОНЧАНИЕ ЗАЩИТЫ	
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Окончание защиты имеет контрольный номер 1
ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	10
РЕЗУЛЬТАТ ЗАЩИТЫ	Цифровая подпись сообщения.
РЕЗУЛЬТАТ ПРОВЕРКИ ПОДЛИННОСТИ Квалификатор контрольного значения Контрольное значение	 Уникальное контрольное значение: 1. 512-битовая цифровая подпись

Приложение D
(справочное)
Функции фильтрации для наборов графических знаков UN/EDIFACT уровней A и C

D.1 Фильтр EDA

D.1.1 Обоснование

Шестнадцатеричная фильтрация удваивает число знаков, необходимых для представления двоичных данных. Область отображения такой функции является избыточной. Однако другие известные стандартизованные функции фильтрации либо просто не применимы для наборов графических знаков UN/EDIFACT уровней A и B (ИСО/МЭК 646) из-за отображения такими фильтрами почти на полный набор печатных знаков ИСО (94 из 96), либо их эффективность в части области отображения не выше, чем у шестнадцатеричной фильтрации (фильтр Бодо).

С учетом этого рекомендуется выбирать такую функцию фильтрации, которая является достаточно простой и отображает двоичные данные на некоторое подмножество набора графических знаков UN/EDIFACT уровня A, и одновременно была бы более эффективна по сравнению с шестнадцатеричным фильтром.

D.1.2 Наборы графических знаков UN/EDIFACT

Набор графических знаков уровня A содержит 44 знака неограниченного использования. Дополнительно к 44 знакам в набор A входят четыре служебных знака и восемь знаков, не используемых при передаче по каналам телекса.

Все эти знаки являются также частью набора графических знаков UN/EDIFACT уровня B, который не предназначен для передачи по каналам телекса и содержит 82 обычных и три непечатаемых служебных знака.

D.1.3 Фильтрация путем замены двух знаков тремя

Для представления двух двоичных знаков тремя знаками в результате фильтрации необходимо иметь в наборе не менее 41 знака: $41 ** 3 = 68\,921 > 65\,536 > 64\,000 = 40 ** 3$.

D.1.4 Описание фильтра EDA

В данном фильтре используются 44 разрешенных знака; для исключения знака пробела из входного набора выделяется и отфильтровывается каждая пара знаков индивидуально (непарный входной знак фильтруется путем представления его только двумя выходными знаками) следующим образом:

— двоичное значение целого числа без знака представляют парой знаков. Это значение зависит от представления чисел в используемом компьютере: какой байт стоит первым – самый младший либо самый старший из значащих[1)]. Стандартное представление чисел предполагает, что первый байт является самым старшим значащим[2)];

— полученное значение представляют последовательностью из трех (а последний нечетный байт – из двух) чисел в диапазоне от 0 до 42; этими числами являются:

— результат деления на 1849 (43 в квадрате) (если последний байт является нечетным, число отсутствует);

— значение по модулю 1849, разделенное на 43;

— значение модуля 43;

— каждый знак алфавита UN/EDIFACT уровня A отображают с помощью таблицы соответствия:

цифры от 0 до 9	представляются цифрами от 0 до 9;
буквы от A до Z	представляются числами от 10 до 35;
знаки ( ) , - . / =	представляются числами от 36 до 42 в установленном порядке.

D.1.5 Дефильтрация

При дефильтрации[1)] выполняют следующие действия:

- каждый из 43 знаков отображают обратно на диапазон значений от 0 до 42,

- если в конце остаются три отфильтрованных знака, то вычисляют короткое целое число, равное $c1 * 1849 + c2 * 43 + c3$;

[1)] В англоязычной документации указанные два варианта представления чисел имеют условные обозначения LITTLE_ENDIAN и BIG_ENDIAN соответственно.

[2)] Условное обозначение – BIG_ENDIAN.

[1)] Обратное преобразование для функции фильтрации.

- в случае когда в конце остаются два отфильтрованных знака вычисляют значение знака, равное c1 * 43 + c2.

Пояснения:

a) результирующее короткое целое число должно быть меньше 65 536,

b) код результирующего знака должен быть меньше 256;

c) при использовании компьютера с порядком следования байтов в представлении чисел начиная с младшего значащего байта (формат представления LITTLE_ENDIAN) два знака короткого целого числа меняются местами.

D.2 Фильтр EDC

D.2.1 Обоснование

Фильтр EDA разработан в целях обеспечения фильтрации с отображением на набор графических знаков EDIFACT уровня A или B. Однако поскольку оба этих набора сильно ограничивают возможный выбор знаков, получаемое в результате относительное расширение (3/2) является плохим результатом, но лучшим, чем при шестнадцатеричной фильтрации (2/1).

Существенное улучшение степени расширения легко достичь в случае использования наборов графических знаков EDIFACT уровней C, D, E и F. В этих наборах единственными запрещенными комбинациями являются двоичные значения от 0/0 до 1/15 и от 8/0 до 9/15, благодаря чему из 256 возможных двоичных значений разрешенными оказываются 192.

Фильтр уровня C идеален по своему низкому показателю расширения, но требует проведения длительных вычислений и, обеспечивая представление 18 двоичных байтов 19-ю отфильтрованными байтами, не предоставляет возможности преобразовать 19 двоичных байтов в 20 отфильтрованных байтов, так как:

192**19 > 256**18 и

192**20 < 256**19.

Из-за такого ограничения манипуляций с битами на практике удается достичь коэффициента расширения не лучше 8/7.

D.2.2 Преобразование фильтрации

Для преобразования двоичной строки байтов в набор графических знаков уровня C необходимо:

— разбить строку на семибайтовые подстроки (последняя подстрока должна быть длиной не более семи байтов),

— перед каждой подстрокой добавить управляющий байт с начальным значением 64 (бит 1 = 1),

— установить в состояние «1» каждый бит управляющего байта, находящийся в 0-вом разряде или в разрядах со 2-го по 7-й, в зависимости от того, применяется или не применяется фильтрационное преобразование к соответствующему байту данных подстроки,

— для каждого байта данных (databyte) подстроки проверить, следует ли применять фильтрационное преобразование путем выполнения следующих действий:

— проверить, выполняется ли тождество для результата логического умножения байта данных на 64 (databyte .and. 64 == 0)?

— если тождество выполняется, то установить в единицу бит 1 байта данных и соответствующий позиционный бит управляющего байта,

— иначе оставить байт данных и управляющий байт без изменений.

Примечание

— во всех отфильтрованных значениях бит 1 каждого байта должен быть равен 1,

— таким способом из набора графических знаков целевого фильтра исключаются служебные знаки, используемые по умолчанию.

D.2.3 Дефильтрационное преобразование

Для обратного преобразования отфильтрованной строки в двоичную строку необходимо:

- разбить строку на восьмибайтовые подстроки (последняя подстрока должна быть длиной не более восьми байтов),

- рассматривать каждый стартовый байт каждой подстроки как управляющий байт, а остальные – как байты данных,

- проверить разряд 0 и разряды со 2-го по 7-й управляющего байта,

- позиции ассоциируемых байтов в подстроке – с 1-й по 7-ю, соответственно,

- если бит управляющего байта равен 0, то оставить байт данных в соответствующей позиции без изменения,

- если бит управляющего байта равен 1, то установить бит 1 соответствующего байта данных в ноль.

Приложение Е
(справочное)

Службы и алгоритмы защиты

Е.1 Цель и область применения

В настоящем приложении приведены примеры возможных комбинаций элементов данных и значений кодов в группах сегментов защиты. Примеры выбраны для иллюстрации широко используемых методов защиты, разработанных на основе международных стандартов.

Полный набор комбинаций является слишком широким для включения в данное приложение. Приведенные алгоритмы и режимы шифрования не являются обязательными. Пользователь должен сам выбрать методы, адекватные предполагаемым угрозам безопасности.

Цель данного приложения – предоставить пользователю, уже выбравшему методы защиты, универсальную отправную точку для разработки решения, подходящего для конкретной задачи.

Для обеспечения лучшего восприятия и понимания данное приложение разбито на два раздела, в каждом из которых внимание сосредоточено на основных принципах использования защиты.

Два набора комбинаций включают:

1) комбинации с использованием симметричных алгоритмов и встроенных сегментов защиты;

2) комбинации с использованием асимметричных алгоритмов и встроенных сегментов защиты.

Перечень кодов, используемых в матрицах (подмножество полного перечня кодов)

0501	Служба защиты, кодированная	0505	Функция фильтрации, кодированная
1 2 3	Неотказуемость источника Аутентификация источника сообщения Целостность	6	Фильтр EDC UN/EDIFACT

0523	Область применения алгоритма, кодированная	0525	Криптографический режим, кодированный
1 2 3 4 6	Хеширование владельцем Симметричное шифрование владельцем Подпись органом сертификации (CA) Хеширование органом сертификации (CA) Подпись владельцем	16	DSMR (Digital Signature with Message Recovery) – Цифровая подпись с восстановлением сообщения

0527	Алгоритм, кодированный	0531	Квалификатор параметра алгоритма
1	DES (Data Encryption Standard) – стандарт шифрования данных	5	Зашифрованный симметричный ключ
		9	Имя симметричного ключа
8	SHA (Secure Hashing Algorithm) – защитный алгоритм хеширования	10	Имя ключа шифрования ключей
		12	Модуль
		13	Экспонента
10	RSA (Rivest, Shamir, Adleman) – алгоритм Ривеста-Шамира-Адлемана	14	Длина модуля
		25	Параметр P алгоритма DSA
11	DSA (Digital Signature Algorithm) – алгоритм цифровой подписи	26	Параметр Q алгоритма DSA
		27	Параметр G алгоритма DSA
16	SHA1 (Secure Hashing Algorithm) – защитный алгоритм хеширования	28	Параметр Y алгоритма DSA
37	MAC (Message Authentication Code) – код аутентификации сообщения		
38	DIM1 (DataIntegrityMechanism) – механизм обеспечения целостности данных		
40	MDC2 (Modification Detection Code) – код обнаружения модификации		
42	HDS2 (Hash functions) – хеш-функции		

0563	Квалификатор контрольного значения	0577	Квалификатор стороны защиты
1	Уникальное контрольное значение	1	Отправитель сообщения
2	Параметр r алгоритма DSA	2	Получатель сообщения
3	Параметр s алгоритма DSA	3	Владелец сертификата
		4	Аутентифицирующая сторона

Используемые сокращения

a, b, c, d, e – представления контрольного номера защиты;
CA – орган сертификации;
Enc-Key – зашифрованный ключ;
G – параметр G открытого ключа алгоритма DSA;
Hash – значение хеш-функции;
KEK-N – имя ключа шифрования ключей;
Key-N – имя ключа;
KN – имя ключа;
MAC – код аутентификации сообщения;
Mod – модуль;
Mod-L – длина модуля;
P – параметр P открытого ключа алгоритма DSA;
PK/CA – открытый ключ органа сертификации;
Pub-K – открытый ключ;
Q – параметр Q открытого ключа алгоритма DSA;
R – результирующее значение параметра r цифровой подписи с использованием алгоритма DSA;
S – результирующее значение параметра s цифровой подписи с использованием алгоритма DSA;
Sig – подпись;
Y – параметр Y открытого ключа алгоритма DSA.

Е.2 Комбинации с использованием симметричных алгоритмов и интегрированных сегментов защиты

Матрица, приведенная в таблице Е.1, устанавливает взаимосвязи для следующих специфических случаев:

- интегрированная защита на уровнях сообщение/пакет/группа/обмен (ИСО 9735-5);
- использование только симметричного алгоритма;
- службы защиты, обеспечивающие аутентификацию источника и целостность контента.

Аутентификация источника сообщения обеспечивается путем присоединения к сообщению кода MAC. Ниже приведены два примера: первый – для алгоритма DES в режиме CBC с секретным ключом, известным получателю сообщения и вызываемым только по имени ключа (этот пример соответствует ИСО 8731-1), а второй пример основан на использовании алгоритма DES в режиме, описанном в стандарте ИСО/МЭК 9797. Необходимый секретный ключ передается зашифрованным по алгоритму DES с помощью ключа шифрования ключей, общего для отправителя и получателя. Этот ключ шифрования ключей вызывается по имени.

Целостность контента обеспечивается использованием хеш-функции, основанной на алгоритме DES в режиме MDC согласно ИСО 10118-2. В этом третьем примере у отправителя и получателя нет общего секретного ключа. Хешированное значение передается без какой-либо защиты, следовательно, эта служба защиты может оказаться недостаточной для обеспечения безопасной передачи сообщения.

Хотя у отправителя и получателя общие ключи, механизмы шифрования заранее не были согласованы; поэтому для всех алгоритмов и режимов шифрования будут использоваться только явные имена.

В таблице Е.1 приведены только поля защиты, связанные с актуальными методами защиты, алгоритмами и режимами шифрования.

Таблица Е.1 – Матрица отношений при использовании только симметричных алгоритмов

Тег	Наименование	S (статус)	R (максимальное число повторов)	Аутентификация источника сообщения по ИСО 8731-1	Аутентификация источника сообщения по ИСО 9797	Целостность контента по ИСО/МЭК 10118-2	Примечания
SG 1		C	99	Один для каждой службы защиты			1
USH	ЗАГОЛОВОК ЗАЩИТЫ	M	1				
0501	СЛУЖБА ЗАЩИТЫ, КОДИРОВАННАЯ	M	1	2	2	3	
0534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	M	1	a	b	c	
0505	ФУНКЦИЯ ФИЛЬТРАЦИИ, КОДИРОВАННАЯ	C	1	6	6	6	
S500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ	C	2				
0577	Квалификатор стороны защиты	M		1	1	1	2
0538	Имя ключа	C		Key-N	—	—	3
S500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ	C	2				
0577	Квалификатор стороны защиты	M		2	2	2	4
USA	АЛГОРИТМ ЗАЩИТЫ	C	3				
S502	АЛГОРИТМ ЗАЩИТЫ	M	1				
0523	Область применения алгоритма, кодированная	M		2	2	2	
0525	Криптографический режим, кодированный	C		—	—	—	
0527	Алгоритм, кодированный	C		37	38	40	
S503	ПАРАМЕТР АЛГОРИТМА	C	9		Один для имени ключа шифрова-ния ключей		
0531	Квалификатор параметра алгоритма	M		—	10	—	5

Тег	Наименование	S (статус)	R (максимальное число повторов)	Аутентификация источника сообщения по ИСО 8731-1	Аутентификация источника сообщения по ИСО 9797	Целостность контента по ИСО/МЭК 10118-2	Примечания
0554	Значение параметра алгоритма	M		—	KEK-N	—	
S503	ПАРАМЕТР АЛГОРИТМА	C	9		Один для зашифрованного ключа		
0531	Квалификатор параметра алгоритма	M		—	5	—	6
0554	Значение параметра алгоритма	M		—	Enc-Key	—	
Защищаемые структуры данных (пользовательские сегменты/объекты / сообщения /пакеты /группы)							
SG n		C	99	Один для каждой службы защиты			1
UST	ОКОНЧАНИЕ ЗАЩИТЫ	M	1				
0534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	M	1	a	b	c	
0588	ЧИСЛО ЗАЩИТНЫХ СЕГМЕНТОВ	M	1				
USR	РЕЗУЛЬТАТ ЗАЩИТЫ	C	1				
S508	РЕЗУЛЬТАТ ПРОВЕРКИ	M	2				7
0563	Квалификатор контрольного значения	M		1	1	1	
0560	Контрольное значение	C		MAC	MAC	Hash	8

Примечания

1 Обе структуры должны иметь одинаковое число вхождений.

2 Отправитель сообщения.

3 Имя секретного ключа, общего для отправителя и получателя.

4 Получатель сообщения.

5 Ключ шифрования ключей используется отправителем и получателем и вызывается по имени.

6 Секретный ключ передается зашифрованным по алгоритму DES с помощью ключа шифрования ключей.

7 Некоторые алгоритмы подписи (такие как DSA) требуют наличия двух результирующих параметров.

8 Результирующие значения параметра целостности не защищены и могут нуждаться в передаче по отдельному каналу.

Е.3 Комбинации с использованием асимметричных ключей и интегрированных сегментов защиты

В матрице таблицы Е.2 установлены связи для следующих конкретных ситуаций:

- интегрированная защита на уровнях сообщений / пакетов / групп / обмена (ИСО 9735-5);
- предоставляемые службы защиты – неотказуемость источника, два метода с разными способами вычисления цифровой подписи;
- используются два асимметричных алгоритма: RSA и DSA;
- выбираются две хеш-функции: DES в режиме MDC совместно с RSA и SHA-1 совместно с DSA;
- предполагается, что обмен сертификатами ранее не выполнялся;
- в сегменте USC явно идентифицированы хеш-функция и функция для вычисления подписи, используемые органом сертификации для подписи сертификата. Открытый ключ этого органа, необходимый для проверки сертификата подписи, известен получателю. На него есть ссылка по имени в сегменте USC;
- прилагается только один сертификат; второй нужен лишь в том случае, если используется открытый ключ получателя.

Таблица Е.2 – Матрица отношений при использовании асимметричных алгоритмов

ТЕГ	Имя	S	R	Неотказуемость источника (RSA)	Неотказуемость источника (DSA)	Примечания
G 1			9	Один для каждой службы защиты		
SH	ЗАГОЛОВОК ЗАЩИТЫ					
501	СЛУЖБА ЗАЩИТЫ, КОДИРОВАННАЯ			1	1	2
534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ			d	e	
505	ФУНКЦИЯ ФИЛЬТРАЦИИ, КОДИРОВАННАЯ			6	6	
500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ					
577	Квалификатор стороны защиты			1	1	3
500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ					
577	Квалификатор стороны защиты			2	2	4
SA	АЛГОРИТМ ЗАЩИТЫ					
502	АЛГОРИТМ ЗАЩИТЫ					
523	Область применения алгоритма, кодированная			1	1	5
525	Криптографический режим, кодированный			—	—	
527	Алгоритм, кодированный			42	16	
G 2				Только один: сертификат отправителя		
SC						
536	УЧЕТНЫЙ НОМЕР СЕРТИФИКАТА			Учетный номер данного сертификата		
500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ			Владелец сертификата		
577	Квалификатор стороны защиты			3	3	6
500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ			Проверяющая сторона		
577	Квалификатор стороны защиты			4	4	7
538	Имя ключа			Имя РК/СА	Имя РК/СА	
SA	АЛГОРИТМ ЗАЩИТЫ			Функция подписи отправителя		
502	АЛГОРИТМ ЗАЩИТЫ					
523	Область применения алгоритма, кодированная			6	6	8

ТЕГ	Имя	S	R	Неотказуемость источника (RSA)	Неотказуемость источника (DSA)	Примечания
525	Криптографический режим, кодированный			16	—	
527	Алгоритм, кодированный			10	11	
503	ПАРАМЕТР АЛГОРИТМА			Длина модуля	Параметр DSA(P)	
531	Квалификатор параметра алгоритма			14	25	
554	Значение параметра алгоритма			Mod-L	P	
503	ПАРАМЕТР АЛГОРИТМА			Модуль	Параметр DSA(Q)	
531	Квалификатор параметра алгоритма			12	26	
554	Значение параметра алгоритма			Mod	Q	
503	ПАРАМЕТР АЛГОРИТМА			Открытая экспонента	Параметр DSA(G)	
531	Квалификатор параметра алгоритма			13	27	
554	Значение параметра алгоритма			Pub-K	G	
503	ПАРАМЕТР АЛГОРИТМА			—	Параметр DSA(Y)	
531	Квалификатор параметра алгоритма			—	28	
554	Значение параметра алгоритма			—	Y	
SA	АЛГОРИТМ ЗАЩИТЫ			Хеш-функция CA для подписи сертификата		
502	АЛГОРИТМ ЗАЩИТЫ					
523	Область применения алгоритма, кодированная			4	4	9
525	Криптографический режим, кодированный			11	—	
527	Алгоритм, кодированный			1	8	
SA	АЛГОРИТМ ЗАЩИТЫ			Функция генерации подписи CA для подписи сертификата		
502	АЛГОРИТМ ЗАЩИТЫ					
523	Область применения алгоритма, кодированная			3	3	10
525	Криптографический режим, кодированный			16	—	
527	Алгоритм, кодированный			10	11	

ТЕГ	Имя	S	R	Неотказуемость источника (RSA)	Неотказуемость источника (DSA)	Примечания
SR	РЕЗУЛЬТАТ ЗАЩИТЫ	C	1			
508	РЕЗУЛЬТАТ ПРОВЕРКИ	M	2			11
563	Квалификатор контрольного значения	M		1	2	
560	Контрольное значение	C		Sig	R	
508	РЕЗУЛЬТАТ ПРОВЕРКИ	M	2			11
563	Квалификатор контрольного значения	M		—	3	
560	Контрольное значение	C		—	S	
Защищаемые структуры данных (пользовательские сегменты/объекты /сообщения/пакеты /группы)						
G n		C	99	Один для каждой службы защиты		1
ST	ОКОНЧАНИЕ ЗАЩИТЫ	M	1			
534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	M	1	d	e	
588	ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	M	1			
SR	РЕЗУЛЬТАТ ЗАЩИТЫ	C	1			
508	РЕЗУЛЬТАТ ПРОВЕРКИ	M	2			11
563	Квалификатор контрольного значения	M		1	2	
560	Контрольное значение	C		Sig	R	
508	РЕЗУЛЬТАТ ПРОВЕРКИ	M	2			11
563	Квалификатор контрольного значения	M		—	3	
560	Контрольное значение	C		—	S	

ТЕГ	Имя	S	R	Неотказуемость источника (RSA)	Неотказуемость источника (DSA)	Примечания

Примечания

1 Обе структуры должны иметь одинаковое число вхождений.

2 Предполагается, что служба аутентификации источника сообщения и служба сохранения целостности включены в службу неотказуемости источника.

3 Отправитель сообщения.

4 Получатель сообщения.

5 Хеш-функция, значение которой вычислено отправителем для защищаемой структуры.

6 Владелец сертификата: идентификационные элементы должны быть теми же, что и в USH S500 для отправителя сообщения.

7 Проверяющая сторона: орган сертификации (CA).

8 Функция генерации подписи отправителя.

9 Хеш-функция CA.

10 Функция генерации подписи CA.

11 Некоторые алгоритмы подписи (например, DSA) требуют наличия двух результирующих параметров.

Приложение ДА
(справочное)
Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 9735-1:2002	IDT	ГОСТ Р ИСО 9735-1–2012
ИСО 9735-2:2002	IDT	ГОСТ Р ИСО 9735-2–2012
ИСО 9735-6:2002	IDT	ГОСТ Р ИСО 9735-6–2012
ИСО 9735-7:2002		*
ИСО 9735-8:2002		*
ИСО 9735-10:2002		*
ИСО/МЭК 10181-2:1996		*
ИСО/МЭК 10181-4:1997		*
ИСО/МЭК 10181-6:1996		*

* Соответствующий национальный стандарт отсутствует (в разработке). До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание – В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

IDT – идентичные стандарты.

Библиография

[1] ИСО/МЭК 646:1991 Информационные технологии. 7-битный набор кодированных знаков ИСО для обмена информацией (ISO/IEC 646:1991, Information technology — ISO 7-bit coded character set for information interchange)

[2] ИСО 8601:2000[1] Элементы данных и форматы для обмена информацией. Обмен информацией. Представление дат и времени (ISO 8601:2000, Data elements and interchange formats — Information interchange — Representation of dates and times)

[3] ИСО 8731-1:1987[2] Банковское дело. Утвержденные алгоритмы для аутентификации сообщений. Часть 1. Алгоритм кодирования данных (DEA) (ISO 8731-1:1987, Banking — Approved algorithms for message authentication — Part 1: DEA)

[4] ИСО/МЭК 9797:1994[3] Информационные технологии. Методы защиты. Механизм целостности данных с использованием функции криптографического контроля на основе алгоритма блочного шифрования (ISO/IEC 9797:1994, Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm)

[5] ИСО/МЭК 10116:1997[4] Информационные технологии, Методы обеспечения безопасности. Режимы работы для n-битовых блочных шифров (ISO/IEC 10116:1997, Information technology — Security techniques — Modes of operation for an n-bit block cipher)

[6] ИСО/МЭК 10118-2:2000[5] Информационные технологии. Методы защиты информации. Хэш-функции. Часть 2. Хэш-функции с использованием алгоритма шифрования n-битовыми блоками (ISO/IEC 10118-2:2000, Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher)

[7] ИСО/МЭК 10181-1:1996 Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Часть 1 Обзор (ISO/IEC 10181-1:1996, Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview)

[8] ИСО/МЭК 10646-1:2000[6] Информационные технологии. Универсальный многооктетный набор кодированных знаков. Часть 1. Архитектура и основная многоязычная матрица (ISO/IEC 10646-1:2000, Information technology — Universal Multiple-Octet Coded Character Set (UCS) — Part 1: Architecture and Basic Multilingual Plane)

[9] ИСО/МЭК 11770-1:1996[7] Информационные технологии. Методы защиты. Управление ключами. Часть 1. Структура (ISO/IEC 11770-1:1996, Information technology — Security techniques — Key management — Part 1: Framework)

---

[1] На момент утверждения настоящего стандарта действует ИСО 8601:2004.
[2] Отменен.
[3] Отменен.
[4] На момент утверждения настоящего стандарта действует ИСО/МЭК 10116:2006.
[5] На момент утверждения настоящего стандарта действует ИСО/МЭК 10118-2:2010.
[6] Отменен.
[7] На момент утверждения настоящего стандарта действует ИСО/МЭК 11770-1:2010.

УДК 658.6/.9:002.006.354 ОКС 35.240.60

Ключевые слова: электронный обмен данными, синтаксические правила, EDIFACT

Подписано в печать 01.04.2014. Формат 60x84 1/8.
Усл. печ. л. 5,12. Тираж 48 экз. Зак. 2921
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»
123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru